Abstract of the Disclosure

A method for dynamically changing an intrusion detection rule in a kernel level intrusion detection system is disclosed. The method includes the steps of: a) generating a replica of the intrusion detection rule in a kernel area; b) changing the replica of the intrusion detection rule according to a request of changing the intrusion detection rule from the kernel area; and c) changing a currently applied intrusion detection rule by exchanging a value of a pointer representing the intrusion detection rule with a value of a pointer representing the changed replica of the intrusion detection rule.